UNIS NGIPS 8000[T1000-CN-G][T1000-E]系列入侵防御系统

故障处理手册

目 录

1 部署方式故障处理

1.1 旁路模式无法对流量进行监听

1.1.1 故障描述

查看设备监控日志无相应日志显示。

1.1.2 故障处理步骤

(1) 查看用户 IP 地址信息，无错误配置。

(2) 检查旁路模式接口启用情况。

(3) 查看用户地址对象匹配的网段是否正确。

(4) 检查安全策略是否被匹配。

1.1.3 故障诊断命令

表1-1 故障诊断命令

命 令	说明
display interface	查看当前接口IP信息及接口状态
display running-config interface	查看当前接口是否设置为旁路模式（deploy-mode listen enable）
display running-config policy	查看设备安全策略是否匹配及策略行为（permit/deny）
display address	查看地址对象网段是否正确匹配

2 升级异常维护指导

版本升级包括软件和特征库文件升级，升级的方式存在多种，在不同场景的实际应用中，可能会存在多种多样的问题，下面详细介绍一下系统升级管理员实际操作中的故障定位思路和方法。

2.1 主程序升级常见问题定位方法

进行主程序升级，常见问题包括：

- Web 界面下无法正常升级
- 命令行界面下无法正常升级
- Menuboot 下无法正常升级

下面将详细介绍各种常见问题的定位方法。

2.1.1 Web 界面下无法正常升级

(1) 首先检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）

(2) 检查升级文件是否正确，版本文件必须以.bin 为后缀名。版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 确保上传升级文件过程中网络正常，设备端需要提示上传成功。

(4) 升级文件上传成功后需要进行设备配置保存操作。

2.1.2 命令行界面下无法正常升级

(1) 首先检查线路连通性，确定线路按照拓扑相连。确定 Console 线路无损坏， 连接设备端口正确。

(2) 检查升级文件是否正确，版本文件必须以.bin 为后缀名。版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 确定 TFTP 和 FTP 服务器正常，文件服务器路径设置正确。文件服务器登录名，密码与命令设置相同。

(4) 检查命令是否输入正确。

(5) 确保升级完成后 设备重启，用 **display version** 命令检查版本信息：

2.1.3 Menuboot 下无法正常升级

(1) 首先检查线路连通性，确定线路按照拓扑相连。确定 Console 线路无损坏， 连接设备端口正确。

(2) 检查升级文件是否正确，版本文件必须以.bin 为后缀名。版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 若设备无 CF 卡或 CF 卡中 menuboot 程序损坏，则需要在其它设备导入 menuboot 文件，例如，可以在连接设备的管理员 PC 上安装 3Cdemon 文件服务器，在 menuboot 中通过 **setenv** *serverip*，**setenv** *ipaddr*，**setenv loadfile** *menuboot.bin* 三个命令，分别设置文件服务器的 IP 地址，设备 IP 地址，与加载 menuboot 文件。

(4) 检查 menuboot 中各参数是否设置正确。

2.1.4 其它问题

其它问题如网线等物理层问题导致升级失败的请注意检查，如有其它问题请联系设备售后人员或咨询售后服务电话。

2.2 特征库升级常见问题定位方法

设备系统在线运行时需要周期性的更新特征库，才能更好进行应用识别控制和流量控制。在设备无法正常与互联网进行通信的情况下，可通过 WEB 页面进行特征库手动升级。若设备可正常与互联网进行通信，则可通过设置定期自动从服务器更新最新的特征库。

2.2.1 手动升级

(1) 首先检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）

(2) 检查升级文件是否正确，版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 确定在上传进度条完成后，WEB 界面提示上传成功，然后进行的下一步操作。

2.2.2 自动升级

(1) 自动升级需要设备接入互联网，检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）。

(2) 检查升级文件是否正确，版本文件是从官网或者正规渠道获得的正确的升级文件。

(3) 检查外网线路网络质量是否正常，检查设备 DNS 是否正确配置，若无配置，请将主备正确设置。

(4) 检查系统升级服务器，设定周期是否设置正常。

2.2.3 其它问题

特征库升级的前提是已经购买并导入授权升级许可，如未购买则无法进行升级，购买授权许可证可以联系厂商相关销售人员。

如有其它问题请联系咨询售后人员。

3 远程控制异常维护指导

不同场景的实际应用中，可能会存在多种多样的问题，下面详细介绍一下系统升级管理员实际操作中的故障定位思路和方法。

3.1 Web管理常见问题定位方法

(1) 检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）

(2) 管理员 IP 与设备 IP 需要在同一网段下。

(3) 需要按照管理员需求，需改接口的访问权限，访问权限参考如下：

- https：允许 HTTPS 访问管理
- http：允许 HTTP 访问管理
- ssh：允许使用 SSH 方式管理
- telnet：允许使用 Telnet 设备管理地址访问管理
- ping：允许 Ping 此接口地址，如果不勾选，路由可达情况下 Ping 不通

(4) 检查浏览器是否正常。

3.2 命令行下管理常见问题定位方法

(1) 检查线路连通性，确定线路按照拓扑相连。确定 Console 线路无损坏， 检查 Console 线两端连接设备端口正确。

(2) 检查管理员 PC 的 COM 端口是否正常。

(3) 检查超级终端配置正确，检查配置协议正确为“serial”，检查波特率配置正确为 9600。

(4) 连接建立后按回车打印显示信息。

3.3 其它问题

如有其它问题请联系设备售后人员或咨询售后服务电话。

3.4 常用调试命令

表3-1 常用调试命令

命令	使用说明
enable	进入特权模式
configure terminal	进入全局配置模式
display running-config	查看所有配置(空格键翻页)
save config	保存当前配置
erase startup-config	恢复出厂配置，需重启设备才能生效
reboot	重启系统，重启前会提示是否保存当前配置
display version	查看版本信息、系统运行时间、设备序列号/型号、功能授权状态等信息
display date	查看系统当前时间(local time)
display interface	查看接口相关信息，包括IP地址、链路状态、MAC地址和工作模式
display cpu usage	查看设备cpu使用率(当前值、1分钟/5分钟/15分钟平均值
display memory	查看设备内存使用率(控制面、数据面)

4 系统资源异常

4.1 CPU0利用率过高

4.1.1 CPU 资源分配机制说明

- 4 核及以下设备转发会使用 0 核，其它设备 0 核仅用来管理。
- 到本地的报文都是 0 核处理。
- 当 0 核参与转发时，优先使用 0 核，这样就会看到 0 核 cpu 比较高。

4.1.2 故障描述

设备在使用时出现卡顿情况，无法操作或者操作等待时间较长，平均 CPU 利用率未达到极限。

通过命令 display cpu usage 查看 CPU 利用情况，发现 CPU0 的利用率达到近 100%，其它 CPU 核利用率不高。

4.1.3 故障处理步骤

(1) 通过命令 display ip connection statistics dest-ip any，查看到本地的报文是否过多，排在前面的目的 IP，有没有是设备接口 IP。

(2) host(config)# local unlistened drop enable，配置非监听端口丢包，将非监听端口的报文丢掉，不让 cpu 进行处理。关闭外网口不必要的管理方式，如非特殊需要，外网口只允许 ping 操作。

(3) 如未解决，收集设备信息、配置文件、perf top 信息，联系售后工程师处理。

4.2 带硬盘的设备看不到审计日志页面

4.2.1 故障描述

带有硬盘的产品在设备首页看不到硬盘的使用率，没有审计日志页面。

4.2.2 故障处理步骤

(1) 通过 recover database 重置数据库，重启设备，看是否恢复正常

(2) 如第(1)步无法恢复，则收集设备启动时串口输出的信息，联系售后工程师处理。

5 应用识别与审计故障处理

5.1 应用识别模式导致审计无法正确识别出应用特征

5.1.1 故障描述

查看应用识别或应用统计集，查看不到正确的应用

5.1.2 故障处理步骤

(1) 执行 **display app-ident mode** 查看是否模式为关闭

(2) 如果性能条件允许修改识别模式为 smart

5.2 网站日志无法记录

5.2.1 故障描述

访问网站，在 web 页面查看网站审计日志，未能查询到对应日志。

5.2.2 故障处理步骤

(1) 页面是否带有 content-type，类型是否为 text/html。

(2) HTTP 返回码是否为 200。

(3) 网页标题长度仅记录为 128 字符范围内（约为 40-60 个汉字）。

(4) URL 长度是否小于 512。

5.3 应用识别与审计不报日志

5.3.1 故障描述

配置应用审计策略，在 web 页面查看应用审计日志，未能查询到日志。

5.3.2 故障处理步骤

(1) 执行 **display running policy** 命令，检查应用审计策略是否正确。

(2) 执行 **display log config** 命令，查看应用审计日志是否记录。

(3) 执行 **debug app audit detail** 和 **debug application identify** 两个调试命令后，执行 **display log debug**+具体应用名称，如 **display log debug QQ**，查看应用审计与识别的细节信息，判断是否识别与审计成功。

(4) 通过查看首页应用流量排名统计来查看是否有误识别和漏识别情况。

(5) 执行 **display ip connection protocol** *protocol-name ip* **source** *source-addr* **dest** *dest-addr*，查看特定 IP 地址的会话的会话的 AppName 字段来确认是否为误识别。

5.4 远程syslog服务器收不到日志

5.4.1 故障描述

在本地可以查看到应用审计日志，配置日志服务器后，在 syslog 服务器端未能收到日志。

5.4.2 故障处理步骤

(1) 执行 **display log config** 命令，查看应用审计日志是否发送，日志服务器是否启用，服务器 IP 及端口是否正确。

(2) Syslog 服务器是否启动，端口是否与设备配置一致。

(3) 执行 **display ip route** 命令，查看路由是否正确，ping 服务器地址是否能 ping 通。

5.5 故障诊断命令

表5-1 故障诊断命令

命令	说明
display running policy	显示应用审计策略
display log config	显示日志配置情况
debug app audit detail	应用审计细节信息
debug application identify	应用识别细节信息
display log debug *app-name*	查看特定应用的debug信息
display ip connection protocol *protocol-name* **ip source** *source-addr* **dest** *dest-addr*	查看过滤特定地址的会话
display ip route	查看路由信息

6 QoS 故障处理

6.1 IPQoS带宽限制不生效问题

6.1.1 故障描述

配置了 IPQoS 带宽限制后发现远未达到所限带宽，流量就已不再增长。

6.1.2 故障处理步骤

检查接口配置的接口带宽与运营商提供的实际带宽是否一致，如：运营商提供 20M 带宽，但 QoS 的带宽显示为 50M，此时带宽已被运营商所提供带宽瓶颈所限制。

6.2 IPQoS最大带宽限速不生效

6.2.1 故障描述

配置了 IPQoS 最大带宽限制后发现未达到最大限速，或者超过了所配置限速值。

6.2.2 故障处理步骤

(1) 检查该 IP 是否超过限速的时间，如果只是一个瞬间的超速是正常的。

(2) 检查该 IP 是否在 QoS 白名单中。

(3) 执行 **display run qos-profile** 查看是否有该 IP 队列，正常情况下上下行都有 1 个队列。（或者 **display qos-profile statistics/display qos-profile**，查看数据包在该 QoS 的队列情况）。

(4) 检查设备是否有多个公网出口，而该 IP 只在某一个接口上做了限制。

(5) 若策略中限制的地址为 any，请改为具体 IP 地址。

(6) 每个策略中的地址薄条目数不超过 8 个。

6.3 应用QoS最大带宽限速不生效

6.3.1 故障描述

配置了应用 QoS 最大带宽限制后发现未达到最大限速，或者超过了所配置限速值。

6.3.2 故障处理步骤

(1) 检查是否开启了应用识别。

(2) 检查是否升级为最新应用特征库。

(3) 在统计集中查看该应用识别成何种应用，然后将该应用加入限制。

(4) 对于 FTP 等需要做 ALG 的环境，检查该应用的 ALG 是否做成功。

6.4 报文不受QoS限制

6.4.1 故障描述

报文未受 QoS 限制。

6.4.2 故障处理步骤

(1) 检查是否是本地报文。

(2) 检测报文是否为非 IPv4/IPv6 报文。

(3) 桥二层报文仅受物理接口的 QoS 限制，不受桥的 QoS 限制。

6.5 流量未匹配QoS策略

6.5.1 故障描述

流量未匹配所配置 QoS。

6.5.2 故障处理步骤

QoS 策略中当有多个对象限制时如：“Address”、“Service”、“APP”等时，为匹配所有对象时才可命中该 QoS 策略。

6.6 故障诊断命令

表6-1 故障诊断命令

命令	说明
clear qos-profile statistics	在定位前先删除已存在的数据包统计
display run qos-profile	显示qos的相关配置
display qos-profile	显示qos接口下的详细包数量
debug qos config	debug qos 相关配置
debug qos match	查看流量匹配qos队列
debug qos drop	所丢弃数据包由哪个qos队列丢弃

7 应用路由

7.1 策略路由常见问题定位

7.1.1 配置了策略路由后，还是无法 Ping 通

- 原因可能是地址对象配置错误和下一跳配置错误。
- 解决方法：分清入口和报文源地址对象，并配置正确下一跳地址。

7.1.2 配置了策略路由后，直连接口无法通信

- 原因可能是错误配置了源接口、源地址、目的地址为 any 的策略路由导致。因为策略路由是优于所有其它路由的(包括直连路由)，错误的配置了这条策略路由后，会改变本地始发的数据包的出接口。
- 解决方法：分清入口和报文源地址对象，精确匹配策略路由引用的地址对象，尽量不要使用 any。

7.2 故障诊断命令

表7-1 故障诊断命令

命 令	说明
display ip route	查看当前设备路由表

7.3 故障诊断命令

表7-2 故障诊断命令

命 令	说明
display address	查看地址对象所匹配的网段
display ip route	查看当前设备路由表
display running-config policy	查看策略配置是否正确引入“地址对象”

8 组网特性故障处理

8.1 IPv6常见问题定位方法

8.1.1 IPv6 设备无法 Ping 通对端的地址

1. 故障现象

无法 Ping 通对端的 IPv6 地址。

2. 故障排除

(1) 在 enable 模式下，用 **display ipv6 interface** 命令检查接口配置的 IPv6 地址是否正确，接口状态是否为 up。

(2) 使用 **debug ipv6 packet** 命令打开 IPv6 报文调试开关，根据调试信息进行判断。**display log debug** 查看具体信息。

8.1.2 IPv6 发送前缀路由，对端 PC 无法接收，故障处理

1. 故障现象

发送前缀路由，对端 PC 无法接收到。

2. 故障排除

(1) 首先查看本地网卡是否已经接收到另一个前缀地址，并排查本地网络中是否有发送多个前缀的设备。

(2) 将网卡禁用再启用，再次获取查看。

8.1.3 IPv6 手动隧道无法通信，故障处理

1. 故障描述

手动隧道配置后，无法正常通信。

2. 故障处理步骤

(1) 手动隧道的源地址和目的地址都需要手动配置。

(2) 查看安全策略配置是否正确。

(3) 查看 IPv6 和 IPv4 路由是否正确。

8.1.4 IPv6 6to4 自动隧道无法通信，故障处理

1. 故障描述

6to4 自动隧道配置后，无法正常通信。

2. 故障处理步骤

(1) 首先分析设置的 6to4 隧道采用的地址是否正确，因为这个地址是一个特殊的地址，需要将 IPv4 公网通信接口的 IPv4 地址转化为 16 进制的 IPv6，o 为 2002:A.B.C.D::/64+EUI-64 格式，其中 2002 表示固定的 IPv6 地址前缀，A.B.C.D::/64 表示该 6to4 隧道对应的 32 位全球唯一的 IPv4 源地址，用 16 进制表示（如 1.1.1.1 可以表示为 0101:0101）。2002:A.B.C.D::/64 之后的部分唯一标识了一个主机在 6to4 网络内的位置。要算换一下此 IP 是否正确。

(2) 查看安全策略配置是否正确。

(3) 查看 IPv6 和 IPv4 路由是否正确。

8.1.5 IPv6 ISATAP 自动隧道故障处理

1. 故障描述

IPv6 ISATAP 自动隧道配置后，无法正常通信。

2. 故障处理步骤

(1) 首先要检查 ISATAP 隧道地址是否添写正确，这里的 ISATAP 隧道地址是经过换算得来的，使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的 ISATAP 地址。ISATAP 地址格式为：Prefix(64bit):0:5EFE:ip-address。其中，64 位的 Prefix 为任何合法的 IPv6 单播地址前缀，ip-address 为 32 位 IPv4 源地址，换算成 16 进制后添在 IPv6 的后 32 位中。

(2) 路由前缀是否通信成功，在本地网卡上查看，可在 PC 端使用 wireshak 抓包。

(3) 查看安全策略配置是否正确。

(4) 查看 IPv6 和 IPv4 路由是否正确。

8.2 VRF故障处理

1. 故障描述

VRF 配置后无法通信。

2. 故障处理步骤

按照标准配置手册文档多次检查配置是否正确，例如排查路由、安全策略是否正确。若配置没有问题，错误依然存在，将配置导出并发给技术支援处理。

8.3 动态路由故障处理

8.3.1 OSPFv2 无法建立邻居定位方法

1. 故障描述

OSPF 邻居关系无法正常建立。

2. 故障处理步骤

如果物理连接和下层协议正常，则检查接口上配置的 OSPF 参数，必须保证与相邻路由器的参数一致，区域号相同，网段与掩码也必须一致（点到点与虚连接的网段与掩码可以不同）。

(1) 使用 **display ip ospf neighbor** 命令查看 OSPF 邻居状态。

(2) 使用 **display ip ospf interface** 命令查看 OSPF 接口的信息。

(3) 检查物理连接及下层协议是否正常运行，可通过 ping 命令测试。若从本地设备 Ping 对端设备不通，则表明物理连接和下层协议有问题。

(4) 检查 OSPF 定时器，在同一接口上邻居失效时间应至少为 Hello 报文发送时间间隔的 4 倍。

(5) 如果是 NBMA 网络，则应该使用 **peer** *ip-address* 命令手工指定邻居。

(6) 如果网络类型为广播网或 NBMA，则至少有一个接口的路由器优先级大于零。

8.3.2 OSPFv2 路由信息不正确

1. 故障描述

OSPF 不能发现其它区域的路由。

2. 故障处理步骤

应保证骨干区域与所有的区域相连接。若一台设备配置了两个以上的区域，则至少有一个区域应与骨干区域相连。骨干区域不能配置成 Stub 区域。

在 Stub 区域内的设备不能接收外部 AS 的路由。如果一个区域配置成 Stub 区域，则与这个区域相连的所有设备都应将此区域配置成 Stub 区域。

(1) 使用 **display ip ospf neighbor** 命令查看 OSPF 邻居状态。

(2) 使用 **display ip ospf interface** 命令查看 OSPF 接口的信息。

(3) 使用 **display ip ospf database** 查看数据库的信息是否完整。

(4) 使用 **display running-config ospf** 命令查看区域是否配置正确。若配置了两个以上的区域，则至少有一个区域与骨干区域相连。

(5) 如果某区域是 Stub 区域，则该区域中的所有设备都要配置 stub 命令；如果某区域是 NSSA 区域，则该区域中的所有设备都要配置 nssa 命令。

(6) 如果配置了虚连接，使用 **display ospf vlink** 命令查看 OSPF 虚连接是否正常。

8.3.3 OSPFv2 路由传递问题

1. 故障描述

查看 OSPFv2 邻居关系显示邻居关系已经 full 状态。但无法学习由 OSPF 邻居传递的路由。

2. 故障处理步骤

(1) 查看 OSPF 接口网络类型，保证建立邻居的接口在相同的网络类型内。

(2) 查看 OSPF 进程是否配置了 distribute 路由过滤。

(3) 查看 OSPF 进程是否设置了域间路由汇总 not-advertise 不通过路由。

(4) 查看 OSPF 进程是否设置了重分布路由不通告。

8.3.4 OSPFv3 无法建立邻居定位

1. 故障描述

查看 OSPFv3 邻居关系时无任何显示，无法与相邻设备建立 OSPFv3 邻居关系。

2. 故障处理步骤

(1) 查看双方直连接口 IPV6 地址，确定直连 IPV6 地址在相同网段内。

(2) 查看 OSPFv3 接口，保证建邻接口在相同 area 内。

(3) 检查建邻设备 router-id 是否冲突。

(4) 查看建邻接口 OSPF hello time 和 dead time 相同。

(5) 查看建邻接口 MTU 是否一致，MTU 一致后邻居关系才可到达 full 状态。

8.3.5 OSPFv3 学习路由条目故障处理

1. 故障描述

OSPFv3 邻居关系正常达到 full 状态，但是无法从 OSPFv3 邻居学习其它路由条目。

2. 故障处理步骤

(1) 查看 OSPFv3 口网络类型，保证建立邻居的接口在相同的网络类型内。

(2) 查看 OSPFv3 进程是否设置了域间路由汇总 not-advertise 不通过路由。

(3) 查看 OSPFv3 进程是否设置了重分布路由不通告。

8.4 HA常见问题定位方法

HA 在主备场景下使用时，常见问题包括：

- HA 无法协商
- HA 主备无法切换
- HA 无法同步

下面将详细介绍各种常见问题的定位方法。

8.4.1 HA 无法协商

要求作为 HA 的两台设备为同一个硬件型号、同一软件版本，选择同样的接口作为 HA 接口配置了抢占模式必须在主设备和备设备上分别配置，一台设备配置为抢占主，一台配置为抢占备。否则 HA 无法协商

8.4.2 HA 主备无法切换

- 备设备有接口处于 down 状态。
- 配置了抢占模式的 HA 设备无法手动切换 HA 状态。

8.4.3 HA 无法同步

- 两台设备型号或版本不同，不同型号的设备接口数目可能不一样，这样配置永远不相同。
- 某个需要 License 的模块主设备有而备份设备没有 License 或已过期，这可能导致配置不同。
- 未开启自动同步功能，导致主备配置不同。
- 在 HA 主设备上重启对端的备设备。HA 备设备可能出现配置和主设备冲突，无法同步的情况。这时可以重启备设备，使备设备抛弃错误配置，使用同步过去的最新配置。

8.4.4 HA 常用调试命令

表8-1 HA 常用调试命令

命令	说明
debug ha error	查看HA错误信息
debug ha event	查看HA事件信息
debug ha filesync	查看HA队列信息
debug ha recv	查看HA发包信息
debug ha send	查看HA收包信息
debug ha session	查看HA会话信息
debug ha sync	查看HA同步状态信息
debug ha recv	查看HA发包信息

8.5 HA联动故障处理

8.5.1 故障描述

设备配置 HA 并且关联 track，主备频繁切换。

8.5.2 故障处理步骤

(1) 设备上查看 track 状态主要看超时时间和间隔设备

(2) 设备上 HA 是否配置了自动抢占

(3) Track 超时时间建议配置默认值 10*4

(4) 关闭 HA 抢占

8.6 HA联动无法切换

8.6.1 故障描述

设备配置 HA 并且在主备墙都关联 track，导致主备无法切换。

8.6.2 故障处理步骤

(1) 设备备墙上查看 HA 配置

(2) 设备备墙上查看 HA 所关联 track 状态是否为 Failed

(3) 设备备墙查看引用的 track 对象的探测目标是从哪个接口出去的

(4) 设备备墙在探测目标的接口下配置管理 ip 地址

8.6.3 故障诊断命令

表8-2 故障诊断命令

命 令	说明
display running-config ha	查看HA配置
display track *name*	查看track详细信息

8.7 Bypass故障处理

8.7.1 故障描述

系统异常时、掉电时接口没有切换到 Bypass 状态。

8.7.2 故障处理步骤

正常情况下 Bypass 模块的触发机制分为硬件触发与软件触发，例如当设备没有通电的情况下，Bypass 功能会调整为开启，如果设备一旦通电后，系统启动成功时，Bypass 立即调整为关闭状态。当系统启动成功后，由于系统故障异常会导致重启时，Bypass 功能会调整为开启状态。当系统运行正常，突发掉电情况下，Bypass 软件会调整为开启状态。

(1) 当发现 Bypass 异常，首先需要判断接口是否属于同一 Bypass 接口。

(2) 当判断网线插口属于正确的 Bypass 接口对时，查看当前配置是否为桥模式，因为 Bypass 仅对二层转发生效，不对三层模式生效。

(3) 由于 Bypass 属于芯片集成功能，由于硬件芯片所属环境如潮湿，干燥，静电也会导致芯片异常功能失效。

9 增强功能

9.1 配置会话限制后没有限制效果

9.1.1 故障描述

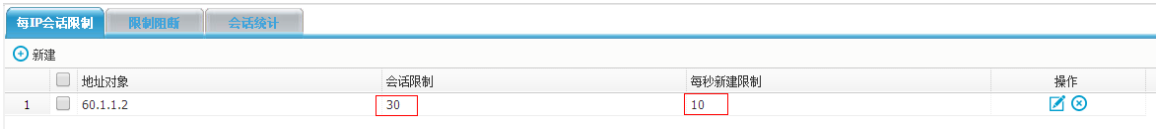
配置了会话限制，但是并没有对配置的地址对象下的会话进行限制。

9.1.2 故障处理步骤

由于配置的地址对象的对应的会话已经建立的数量大于配置的限制的会话数，导致并不能看到会话限制的效果。

比如配置会话限制数为 30，每秒新建限制为 10。

图9-1 会话限制配置



查看限制阻断，没有记录（此时 60.1.1.2 地址对象所对应的流量保持的会话数为 50）。

图9-2 会话限制阻断

查看当前会话统计，60.1.1.2 会话数大于 30。

图9-3 会话统计

如果该地址对象的会话一直有流量的话，会话不会老化，可以在命令下清除当前的会话，即可进行正常的会话限制。如果该地址对象的会话没有流量，可以等候会话老化，之后便能看到会话限制的效果。

```
host# clear ip connection all
```

再查看阻断记录，能够正常阻断。

图9-4 清除会话后的阻断记录

9.1.3 故障诊断命令

表9-1 故障诊断命令

命令	说明
clear ip connection all	清除当前已经建立起来的会话

9.2 DNS代理对客户端请求没有进行处理

9.2.1 故障描述

- 设备开启了 DNS 代理功能，并且配置了 DNS 服务器。
- 客户端配置设备为 DNS 服务器，但是在发出 DNS 请求后收不到响应。

9.2.2 故障处理步骤

查看 CPU 是否过高，DNS 代理的过程通过 CPU0 来处理，CPU0 用作 CP，当 CPU0 偏高时，会产生丢包，执行 **display cpu usage** 命令查看 CPU 占用情况。

查看是否是内存不足导致丢包，设备分配了一定的内存来作为 DNS 请求和转发的缓冲，大小约为 400K，客户端产生大量 DNS 请求时，将导致用于缓冲的内存部分用尽，产生丢包；命令为 **debug dp drop**，**display log debug**。

图9-5 查看是否是内存不足导致丢包

```
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
DNS:Drop dns packet because there is no memory to save it!memory head 408960 tail 408480 size 409600
```

查看是否是 FPA 泄露，FPA 主要负责分配收发报文过程中的 packet work entry 以及 packet 的 data buffer，设备的上的 FPA 存在于 FPA0-FPA3 上，数值会有上下浮动但不会持续下降，当 FPA 泄露完之后导致设备不会转发报文，命令 **display statistics fpa**。

9.2.3 故障诊断命令

表9-2 故障诊断命令

命令	说明
debug dp drop	查看转发过程中的丢包情况
display cpu usage	查看CPU 使用情况
display log debug	查看debug产生的日志
display statistics fpa	查看fpa状态

9.3 无法拦截入侵防御事件攻击

9.3.1 故障描述

配置了入侵防御后发现无法拦截 IPS 攻击流量。

9.3.2 故障处理步骤

(1) 查看事件集是否被策略引用并开启规则。

(2) 查看事件集是否勾选正确。

(3) 查看流量匹配策略是否为配置策略。

9.3.3 故障诊断命令

表9-3 故障诊断命令

命令	说明
debug dp basic	查看流量命中策略
display running-config ips	查看ips配置信息
debug ips detect /event	Debug ips攻击情况/debug ips 攻击事件
debug ip packet receive	debug收到的数据包
debug ip packet send	debug转发的数据包
debug dp filter	设置debug过滤器

9.4 无法拦截 AV 攻击

9.4.1 故障描述

配置了 AV 防护后发现无法拦截 AV 病毒。

9.4.2 故障处理步骤

(1) 是否升级最新病毒库。

(2) 病毒类型是否为 zip 压缩文件。

(3) 是否被策略引用并命中策略。

9.4.3 故障诊断命令

表9-4 故障诊断命令

命令	说明
debug dp basic	查看流量命中策略
display run av	查看av配置信息
debug av event	Debug av 事件记录
debug av file	Debug av 文件
Debug av scan	Debug av 扫描过程

9.5 无法拦截DoS攻击

9.5.1 故障描述

配置了 DoS 攻击防护后发现无法拦截 DoS 攻击流量。

9.5.2 故障处理步骤

(1) 执行 **display running-config defend** 检查设置的 DoS 攻击防护是目的 IP 防御还是接口防御，其中目的 IP 防御是全局生效的，而接口防御仅对被设置的接口生效。

(2) 如果设置的是目的 IP 防御，检查该 IP 是否在设置的保护主机范围内。

(3) 如果设置的是接口防御，该接口是否是 DoS 攻击的入接口。

9.5.3 故障诊断命令

表9-5 故障诊断命令

命令	说明
display statistics interface	查看所有端口的统计信息
display running-config defend	查看安全防护配置信息
debug ip defend attack	debug安全防护丢包信息
debug ip packet receive	debug收到的数据包
debug ip packet send	debug转发的数据包
debug dp filter	设置debug过滤器

9.6 恶意URL白名单故障处理

9.6.1 故障描述

安全策略开启 URL 过滤后，某些网站无法访问，查看恶意 URL 日志，发现网页被阻断。配置了恶意 URL 白名单后重新访问网站还是不能访问。

9.6.2 故障处理步骤

(1) 查看访问的网站 URL 是否填写正确。

(2) 查看恶意 URL 日志，访问的网站是否有记录。

(3) 查看配置的恶意 URL 白名单是否正确，恶意 URL 白名单为精确匹配

(4) 修改恶意 URL 白名单后，重新访问网站

9.6.3 故障诊断命令

命 令	说明
display malware_whitelist	查看恶意URL白名单配置
malware-url *url*	添加恶意URL白名单

9.7 管理员无法登录Web页面

9.7.1 故障描述

无法使用新建的管理员账户登录设备。

9.7.2 故障处理步骤

(1) 查看新建管理员用户名、密码配置（可以使用默认的 admin 账户登录）。

(2) 查看新建管理员是否配置管理 IP 地址。

(3) RADIUS、LDAP 服务器是否正常。

9.7.3 故障诊断命令

表9-6 故障诊断命令

命 令	说明
display amdin-user（管理员名称）	查看设备中该管理员是否存在及用户类型、用户状态、管理地址、管理员权限

9.8 断点续传故障处理

9.8.1 断点续传描述

属于断点续传的有服务器不可达/服务器 down/vtysh 超时退出（这种情况下，属于断点下载范围。当设备版本下载过程中断掉后，再次开始后从上一次的进度处开始下载）

9.8.2 故障描述

- 使用 FTP 方式下载版本文件，版本下载失败
- 使用 HTTP 方式下载版本文件，版本下载失败

9.8.3 故障处理步骤

(1) FTP 服务器是否开启，PC 端需要关闭防火墙。
(2) 查看版本文件是否放在 FTP 服务器正确的目录下。
(3) 查看 FTP 服务器是否设置了登录口令。
(4) 设备端下载版本文件名是否正确。
(5) 下载过程中，用户主动断掉（ctrl+c，这种情况不属于断点下载，需要重头开始下载）。
(6) HTTP 服务器是否开启，PC 端需要关闭防火墙。
(7) 查看版本文件是否放在了 HTTP 服务端的目录下。
(8) 设备端下载版本文件名是否正确。。
(9) 下载过程中，用户主动断掉（ctrl+c，这种情况不属于断点下载， 需要重头开始下载）。

9.9 第三方用户存储认证故障处理

9.9.1 故障描述

设备配置 RADIUS/LDAP 第三方认证后访问外网无法重定向到认证页面。

9.9.2 故障处理步骤

(1) 设备上控制控制策略是否将流量拒绝。
(2) 查看设备上的用户策略是否正确。
(3) 查看设备上的路由配置是否正确。

9.9.3 故障诊断命令

表9-7 故障诊断命令

命 令	说明
display running-config policy	查看设备中控制控制策略
display user-policy	查看设备中用户策略
display ip route	查看设备中路由配置相关信息

9.10 第三方用户存储无法认证成功

9.10.1 故障描述

设备配置 RADIUS/LDAP 第三方认证后，在重定向页面内输入正确的用户名、密码，点击登录，页面提示“用户名或密码错误”。

9.10.2 故障处理步骤

(1) 在命令行 **debug aaa events**，根据相应的 debug 信息查看认证失败的原因，包括服务器没有回应、服务器密码错误、用户名或密码错误。根据这些相应的原因查看是否拓扑或路由错误导致服务器没有回应；RADIUS 服务器密码是否错误；输入的用户名及密码是否正确，此用户在 RADIUS/LDAP 服务器上是否存在。

(2) 查看相应的系统日志，查找故障原因。

9.10.3 故障诊断命令

表9-8 故障诊断命令

命 令	说明
debug aaa events **display log debug**	查看认证失败的相应debug信息
display log event all	查看设备关于认证失败的日志信息

9.11 三权分立

9.11.1 管理员无法登录 WEB 界面问题定位

(1) 检查网络连通性，确定网络线路正常，按照拓扑互联，ping 设备管理 IP 地址可以连通。（接口开启 ping 模式下）

(2) 管理员 IP 与设备 IP 需要在同一网段下。

(3) 需要按照管理员需求，需改接口的访问权限，访问权限参考如下：

- https：允许 HTTPS 访问管理。
- http：允许 HTTP 访问管理。
- ssh：允许使用 SSH 方式管理。
- telnet：允许使用 Telnet 设备管理地址访问管理。
- ping：允许 Ping 此接口地址，如果不勾选，路由可达情况下 Ping 不通。

(4) 检查浏览器是否正常。

9.11.2 系统管理员 Web 登录后看不到任何模块

1. 故障描述

在 Web 登录系统管理员账号后，看不到任何模块。

2. 故障处理步骤

(1) 登录权限管理员账号，查看是否给该系统管理员分配相应模块的权限。

(2) 如果权限管理员只给该系统管理员分配了 CLI 权限，那么登录系统管理员账号也不会显示该模块。

(3) 如果权限管理员只给该系统管理员分配了应用审计日志、网站访问日志模块，当设备没有硬盘时，那么登录系统管理员账号也不会显示该模块。

10 应用/用户流量统计故障处理

10.1 应用/用户流量统计后台数据信息查看方法

后台执行 **display flow-account statistics** 可以查看到后台信息具体内容。

10.1.1 故障诊断命令

表10-1 故障诊断命令举例

命令	说明
display flow-account statistics	查看应用/用户流量统计具体信息内容
WorkState: enabled	当前功能开启
AccountPeriod: 1(centi-seconds)	统计周期为百万分之一秒
UserLost: 0	用户（IP或实名认证用户）没有统计出来的数据会显示在此行
UserTopOut: 0	用户没有进入TOP的数据报文计数
UserTopOldIn: 250	用户首次进入TopN统计的报文数量(N为不同硬件规格规定的上限)
UserTopNewIn: 198	后进入TopN的用户统计的报文数量(将首次进入ToP的数据顶出)
UserOverflow: 0	应用/用户流量统计保存的二维表(用户的应用)用户维度统计溢出计数，另一个是二维表应用维度统计溢出计数
AppLost: 0	用户应用没有统计出来的数据会显示在此行
AppTopOut: 0	应用没有进入TOP的数据报文计数
AppTopOldIn: 322	应用首次进入TOP时的报文计数
AppTopNewIn: 126	后进入TOPN的应用统计报文数量(将首次进入ToP的数据顶出)
AppOverflow: 0	应用/用户流量统计保存的二维表(应用的用户)应用维度统计溢出计数
MemLack: 0	内存分配失败的报文计数

11 地址探测故障处理

11.1 接口联动失败后接口down掉无法up起来

11.1.1 故障描述

设备配置接口联动，track 目标为下一跳地址，在该接口关联 track 对象，track 失败后，接口无法up。

11.1.2 故障处理步骤

(1) 设备上查看接口状是否为 TD（track-down）。

(2) 如果不是 TD 的话查看接口物理线路是否 ok。

(3) 如果是 TD 的话查看 track 对象的下一跳是否为直连接口。

(4) 确定 track 对象下一跳是直连接口后，在接口下删除 track。

11.1.3 故障诊断命令

表11-1 故障诊断命令

命 令	说明
display interface	查看设备接口状态
display running-config interface	查看接口下关联的track
display track *name*	查看track详细信息
display running-config ha	查看HA配置

12 策略故障处理

12.1 无法访问外网

12.1.1 故障描述

设备配置策略后无法访问外网。

12.1.2 故障处理步骤

(1) 是否有去往外网的默认路由。

(2) 设备上控制策略是否将流量拒绝。

12.1.3 故障诊断命令

表12-1 故障诊断命令

命 令	说明
display running-config policy	查看设备中控制策略
display address	查看设备中地址对象
debug policy	查看设备中策略匹配信息
debug app audit detail	查看设备中具体应用规则和URL规则匹配信息

13 IMC 联动故障处理

13.1 无法重定向认证页面

13.1.1 故障描述

设备配置 Portal 认证后访问外网无法重定向 IMC Portal 认证页面。

13.1.2 故障处理步骤

(1) 设备上控制策略是否将流量拒绝。

(2) 查看地址对象是否配置正确。

(3) 用户策略中目的地址是否排除了 IMC 服务器地址、认证方式是否正确。

(4) 设备中 Portal Server 页面的认证 URL 填写是否正确。

13.1.3 故障诊断命令

表13-1 故障诊断命令

命 令	说明
display running-config policy	查看设备中控制策略
display address	查看设备中地址对象
display user-policy	查看设备中用户策略
display running-config user-portal-server	查看设备中Portal Server配置信息

13.2 无法认证成功

13.2.1 故障描述

- 设备配置 Portal 认证后，在重定向页面内输入正确的用户名、密码、服务类型，点击上线，页面报错“设备拒绝请求”。
- 设备配置 Portal 认证后，在重定向页面内输入正确的用户名、密码、服务类型，点击上线，页面报错“向设备发送请求超时”。

13.2.2 故障处理步骤

(1) 查看 Portal Server 配置是否调用了正确的 RADIUS 服务器。

(2) 查看 RADIUS 服务器中服务器地址、服务器密码、端口是否配置正确。

13.2.3 故障诊断命令

表13-2 故障诊断命令

命 令	说明
display running-config user-portal-server	查看设备中Portal Server配置信息
display radius-server	查看设备中RADIUS服务器配置信息

14 用户管理员密码无法登录设备

14.1.1 故障描述

用户忘记管理员密码导致设备无法进行登录管理。

14.1.2 故障处理步骤

(1) 重启设备，按 ctrl+B 进入 menuboot

```
Flash boot bus region not enabled, skipping NOR flash config
PCIe: Port 0 not in PCIe mode, skipping
PCIe: Port 1 not in PCIe mode, skipping
PCIe: Port 2 not in PCIe mode, skipping
PCI console init succeeded, 1 consoles, 1024 bytes each
Press CTRL C to enter menuboot 0
reading menuboot
.....................................................
54850768 bytes read in 9067 ms (5.8 MiB/s)
```

```
================================================================================
******** Please use the interface to communicate ge0********

        ================================================================
        |              BOOT MENU(V4.0-20160122)                        |
        |   1. Upgrade image by FTP.                                   |
        |   2. Upgrade menuboot by FTP.                                |
        |   3. Check and repare file system.                           |
        |   4. Reset administrator passowrd.                           |
        |   5. Producing test.                                         |
        |   6. Aging test.                                             |
        |   7. Display production and aging recored.                   |
        |   8. Advance functions.                                      |
        |   0. Reboot.                                                 |
        |                                                              |
        ================================================================
```

(2) 进入 menuboot 按选项 4，即可重置管理员密码，默认为 admin。显示“Reset admin password success”表示成功。

```
        ================================================================
        |              BOOT MENU(V4.0-20160122)                        |
        |   1. Upgrade image by FTP.                                   |
        |   2. Upgrade menuboot by FTP.                                |
        |   3. Check and repare file system.                           |
        |   4. Reset administrator passowrd.                           |
        |   5. Producing test.                                         |
        |   6. Aging test.                                             |
        |   7. Display production and aging recored.                   |
        |   8. Advance functions.                                      |
        |   0. Reboot.                                                 |
        |                                                              |
        ================================================================

Please input your choice[0-8]:4
Rest admin password success.
```

(3) 选择 0 重启设备

```
        ================================================================
        |              BOOT MENU(V4.0-20160122)                        |
        |   1. Upgrade image by FTP.                                   |
        |   2. Upgrade menuboot by FTP.                                |
        |   3. Check and repare file system.                           |
        |   4. Reset administrator passowrd.                           |
        |   5. Producing test.                                         |
        |   6. Aging test.                                             |
        |   7. Display production and aging recored.                   |
        |   8. Advance functions.                                      |
        |   0. Reboot.                                                 |
        |                                                              |
        ================================================================

Please input your choice[0-8]:0
```

(4) 重新使用 admin 登录即可。

15 流量劫持维护指导

流量劫持的主要问题定位手段是查看流量劫持的配置以及 debug 调试命令。下面详细介绍一下流量劫持在典型应用场景中的故障定位思路和方法。

15.1 流量劫持常见问题定位方法

流量劫持在使用中，常见问题包括：

- 有时候不弹广告页面
- 广告页面弹速度较慢
- 访问网页被重置
- 同一个页面弹出多个广告图片

15.1.1 有时候不弹广告页面

不弹广告页面包括以下几种情况：

(1) 如果访问的是 https 网页，则不支持弹广告页面。

(2) 一个网页多次跳转后广告页面无法弹出原因是同一条连接发起了多个 get 请求只对第一个 get 请求作插入。

其它情况不弹广告页面通过调试命令 **debug http hijack** 查看 http 请求是否匹配到流量劫持。

调试命令：**debug http hijack**

15.1.2 广告页面弹出速度较慢

流量劫持广告弹出与网速带宽、广告过滤软件等都有关，网速慢的情况下图片加载就慢。

调试命令：**debug http hijack**

15.1.3 访问网页被重置

个别网站在开启流量劫持的情况下，网页停留一段时间后，提示网页已重置（网页邮箱）这类网站会定期向服务器端发送请求报文，与流量劫持插入代码冲突，导致网页显示重置，目前没有好的处理办法。建议，在域名白名单排除掉该网站

调试命令：**debug http hijack**

15.1.4 同一个页面弹出多个广告图片

一些网站结构为 frameset 框架布局，主界面里包含多个其它请求，广告图片会显示多个，目前暂无法处理，建议：此类网站加入域名白名单排除掉该网站。

调试命令：**debug http hijack**

16 日志信息收集方式

16.1 日志信息收集方式

16.1.1 故障描述

一些应用出现问题或者设备出现意外重启等问题，都会被日志记录下来（保证设备有硬盘或者充当硬盘的外置 U 盘），那么在排查问题的时候，日志收集是很重要的。

16.1.2 日志收集的方式

(1) 在 web 界面收集。

(2) 收集系统版本信息——web 和命令行。

尽量使用命令行收集，使信息更清晰：**display version**。

(3) 使用 Debug 打印基本信息用来分析。

根据想抓取的应用或者服务进行 debug 调试信息（请参照 debug 手册进行）；通过 **display log debug** 来收集信息。

(4) 从 web 界面收集一些日志信息，尽量找到离事件发生最近的日志来分析，选中可以复制到 Word 文档中，提供给后端人员进行分析。

	时间	日志级别	日志内容
1	2020-07-07 18:09:17	警告	ge0 链路状态变为关闭!
2	2020-07-07 18:05:16	通知	admin@192.168.10.205 登录成功，登录来自于WEB
3	2020-07-07 17:42:48	通知	会话超时，用户 admin@192.168.1.100 退出WEB
4	2020-07-07 17:32:30	通知	admin@192.168.1.100 登录成功，登录来自于WEB
5	2020-07-07 17:32:09	通知	admin@192.168.1.100 登录成功，登录来自于WEB
6	2020-07-07 17:15:12	通知	admin@192.168.1.100 登录成功，登录来自于WEB
7	2020-07-07 16:31:47	通知	会话超时，用户 admin@192.168.1.100 退出WEB

16.1.3 故障诊断命

表16-1 常用命令

命 令	说明
debug dp basic	查看数据的基本处理转发流程
display log debug	查看日志信息